

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

COALITION FOR INDEPENDENT
TECHNOLOGY RESEARCH,
Plaintiff,

v.

No. 1:23-cv-00783

GREG ABBOTT, in his official capacity
as Governor of the State of Texas, et al.
STEVEN C. MCCRAW, in his official
capacity as Director and Colonel of the
Texas Department of Public Safety,
AMANDA CRAWFORD, in her official
capacity as Executive Director of the
Texas Department of Information
Resources and Chief Information Officer
of Texas, DALE RICHARDSON, in his
official capacity as Chief Operations
Officer of the Texas Department of
Information Resources, ASHOK MAGO,
LAURA WRIGHT, LINDY RYDMAN,
CARLOS MUNGUIA, MARY DENNY,
MILTON B. LEE, MELISA DENIS,
DANIEL FEEHAN, and JOHN SCOTT,
JR., in their official capacities as members
of the Board of Regents of the University
of North Texas System, and MICHAEL
WILLIAMS, in his official capacity as
Chancellor of the University of North
Texas System,
Defendants.

DECLARATION OF MEGHAN FRKUSKA

Meghan Frkuska declares:

1. I am the Privacy Counsel and Chief Privacy Officer for the Texas Department of Public Safety (“DPS”). I make this declaration based on my personal observations, knowledge, and

involvement in drafting the January 26, 2023, Model Security Plan for Prohibited Technologies (“Model Plan”) issued by DPS and the Texas Department of Information Resources (“DIR”).

2. I do not believe that any of my following statements reveal legal advice I gave to DPS in connection with the Model Plan or any other matter. I do not intend to waive any privileged communications or other issues through this declaration.

I. TikTok is a Potential Security Threat to Texas State Agencies.

3. TikTok is a potential security threat to Texas state agencies. Numerous media reports show the close ties between TikTok, its Chinese-based parent company ByteDance, and the Chinese Communist Party (“CCP”). These ties create a risk that the CCP can exploit its access to TikTok to invade the privacy of users of this application and to obtain sensitive information about Texas state agencies, employees, and citizens who interact with state agencies or use government services.

4. One significant concern is that the CCP could exploit TikTok to access everything a user does on a TikTok-installed device, like a cellphone. Media reports, cybersecurity websites, and TikTok’s terms of service indicate that TikTok has access to biometric identifiers, keystroke patterns, pasted clipboard information, location information, and app specific usage data. This would potentially allow the CCP to see state employees’ and citizens’ faces and backgrounds (including those who are not on other social media) as well as see, store, and use any state resources that a user accesses with a TikTok-installed device.

5. Another significant concern is that media reports, cybersecurity websites, and TikTok’s terms of service indicate that TikTok can access the camera and microphone on a user’s device. The CCP could reasonably exploit this access to eavesdrop on sensitive conversations held by state employees and any citizens giving sensitive information to state employees to receive government services.

6. As directed, DPS and DIR drafted a model plan for approximately 200 state agencies and institutions of higher education in Texas. These agencies naturally have widely varying missions, data, resources, and access to internal resources for cybersecurity and privacy issues.

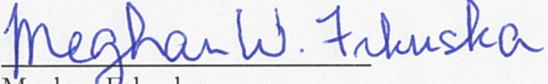
II. The Fact that Some User Data may be Commercially Available does Not Nullify the Security Risks Posed by TikTok.

7. I have reviewed the Declaration of Bruce Schneier that Plaintiff filed during this case.¹ Schneier maintains that “the Chinese government can collect immense volumes of data” through commercial data brokers.² Yet Schneier does not appear to suggest that *all* of TikTok’s data would be commercially available.

8. Commercial data brokers are likely not selling some of the more sensitive and specific data that TikTok collects on its users, such as keystrokes, biometric identifiers, location information, usage data, passwords, financial information, and the content of personal messages.

9. I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 12, 2023


Meghan Prkuska

¹ ECF 20-3.

² *Id.* at ¶¶ 26-30.